

MAR 07 2007

Serial No. 10/764,918
Amendment and Response to Office Action
Mailed December 8, 2006**REMARKS**

In the Office Action, the Examiner rejected claims 1-26, 31, and 32, and indicated claims 27 and 28 as being allowed. Applicant thanks the Examiner for indicating the allowable subject matter. By this paper, claims 1, 2, 8-22, 31 and 32 have been amended to clarify certain aspects of the claimed subject matter. Additionally, dependent claims 33 and 34 have been added to clarify certain aspects of the claimed subject matter. Accordingly, claims 1-28 and 31-34 are pending. In view of the amendments, Applicant respectfully requests reconsideration and allowance of all pending claims.

Claim Rejections under 35 U.S.C. § 101

The Examiner rejected claims 8-20 under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Specifically, the Examiner stated:

Claim 8, 14 direct to a security module which is a software/program (see specification's paragraph 21, lines 1-2). Therefore, the claimed invention is directed to non-statutory subject matter.

Office Action, page 3. Applicant respectfully traverses this rejection.

According to the Supreme Court, Congress intended statutory subject matter to "include anything under the sun that is made by man." *Diamond v. Chakrabarty*, 447 U.S. 303, 308-09; 206 U.S.P.Q. 193, 197 (1980). Indeed, exclusions of statutory subject matter are limited to laws of nature, natural phenomena, and abstract ideas. See *Diamond v. Diehr*, 450 U.S. 175, 185; 209 U.S.P.Q. 1, 7 (1981). Other than these specific exceptions, therefore, nearly anything man made is statutorily patentable subject matter under 35 U.S.C. §101.

Serial No. 10/764,918
Amendment and Response to Office Action
Mailed December 8, 2006

The Federal Circuit has developed a test which may be used to determine if a claim recites statutory subject matter, namely whether the claim produces a “useful, concrete, and tangible result.” *In re Alappat*, 31 U.S.P.Q.2d 1545, 1557 (Fed. Cir. 1994) (*en banc*). The Federal Circuit has stated “the dispositive inquiry is whether the claim *as a whole* is directed to statutory subject matter.” *Id.* The Federal Circuit elaborated by holding that one must look to “the essential characteristics of the subject matter, in particular, its practical utility.” *State Street Bank & Trust Co. v. Signature Financial Group Inc.*, 47 U.S.P.Q.2d 1596, 1602 (Fed. Cir. 1998). Additionally, the Federal Circuit has stated “the *Alappat* inquiry simply requires an examination of the contested claims to see if the claimed subject matter *as a whole* is a disembodied mathematical concept representing nothing more than a ‘law of nature’ or an ‘abstract idea,’ or if the mathematical concept has been reduced to *some practical application rendering it ‘useful’*.” *AT&T Corp. v. Excel Communications, Inc.*, 50 U.S.P.Q.2d 1447, 1451 (Fed. Cir. 1999) (emphasis added). In other words, “Is an actual process machine, manufacture, or composition of matter being claimed in accordance with 35 U.S.C. §101, or is the claim drawn to an abstraction?” Therefore, if a claim, read as a whole and in light of the specification, produces any useful, concrete, and tangible result, the claim meets the statutory requirements of Section 101. *See id.*

Amended independent claims 8 and 14 each recite “a first security module in a computer,” along with associated structure in the bodies of the claims. Specifically, the body of claim 8 recites, “*a detector that is adapted to detect another security module...and a device that obtains at least one key.*” (Emphasis added). The body of claim 14 recites, “*means for detecting another security module...means for determining whether a key associated with the*

Serial No. 10/764,918
Amendment and Response to Office Action
Mailed December 8, 2006

other security module is stored at the first security module; and *means for obtaining* the key.” (Emphasis added). Accordingly, the subject matter of independent claims 8 and 14 clearly *does not* represent a “disembodied mathematical concept representing nothing more than a ‘law of nature’ or an ‘abstract idea,’” but, rather, is directed to an apparatus plainly allowable under 35 U.S.C. § 101. *See AT&T Corp. v. Excel Communications, Inc.*, 50 U.S.P.Q.2d 1447, 1451 (Fed. Cir. 1999). Moreover, the security modules of claims 8 and 14 include the capability to detect another security module and obtain a key, the key providing redundancy of keys should a security module fail. As such, the subject matter of claims 8 and 14 produce concrete, useful, and tangible results and provide practical utility to meet the statutory requirements of Section 101, as set forth above.

With regard to the Examiner’s statement that the security modules are directed to non-statutory subject matter because the security module is software or a computer program, Applicant asserts that software or computer programs are considered patentable subject matter under Section 101 if they are in a tangible medium. Indeed, the Commissioner of Patents stated, “[C]omputer programs embodied in a tangible medium...are patentable subject matter under 35 U.S.C. §101.” *See In re Beauregard*, 53 F.3d 1583 (Fed Cir. 1995). It is clear from the specification that the security modules are in a tangible medium and, further, that they are operated by a microprocessor. *See, e.g.*, FIG. 3. It is simply not accurate or reasonable for the Examiner to assert otherwise. As such, for at least this additional reason, claims 8 and 14 are directed to patentable subject matter.

Accordingly, because independent claims 8 and 14, taken as a whole, recite apparatuses which produces a concrete, useful, and tangible result and, further, because the

Serial No. 10/764,918
Amendment and Response to Office Action
Mailed December 8, 2006

security modules are embodied in a tangible medium, Applicant respectfully asserts that each recites statutory subject matter under 35 U.S.C. § 101. As such, Applicant respectfully requests withdrawal of the rejection under 35 U.S.C. § 101 of independent claims 8 and 14, as well as the rejection of all claims dependent thereon.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected claims 1-26, 31, and 32 under 35 U.S.C. § 103 (a) as being unpatentable over Timson et al (U.S. Patent No. 6,041,412) (hereinafter "Timson") in view of Challenger (U.S. Pub. 2003/0174842) (hereinafter "Challenger"). Specifically, the Examiner stated:

Claims 1-26, 31, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Timson et al (6041412) in view of Challenger (US Pub 2003/0174842). As in claim 1, Timson discloses a method to operating security modules in a computer (Timson's Fig. 1: #2 CPU corresponding to the claim's computer, two security modules (Fig 1: #50, #60, Fig 2: #8, dual secure data modules, column 8, lines 48-65) attaching locally to the computer. Timson does not disclose the claim's detail acts associating with the security modules, However, Challenger '842 describes a method for storing private key of one security in another security module using establish standard such as TCPA (Challenger's paragraph 6, lines 1-10_ comprising the acts of detecting a second security module in the computer; determining whether a key associated with the second security module is available to the first module (Challenger '842's paragraph 28, Fig 3:#54 query whether user's private key is stored on the TCM server, Fig 1: #40 that corresponds to the claim's first security module); and obtaining the key associated with the second security module is the key associated with the second security module is not stored at the first security module (Challenger '842's paragraph 28, server obtains the private key from the client's security module, Fig 1: #54 that corresponds to the claim's second secure module, Fig 1: #22; Challenger's paragraph 12 discloses that the first security module, TCM server Fig 1: #40, obtaining the private key associating with the second security module, Fig 1:#22, and providing this key information to a cline/user. Obviously, if this key has not been stored at the first security module, the first security module,

Serial No. 10/764,918
Amendment and Response to Office Action
Mailed December 8, 2006

server, will obtain it from the client's computer and save it for future referencing, in a migrating manner, see Fig. 4a, paragraph 32).

It would have been obvious to one of ordinary skill in the art at the time of invention to include the method and associating apparatus for storing private key of one security in another security module using establish standard such as TCPA, thereby the private key of one security module can be retrieved from another security safely with any computers enable with established standard such as TCPA (see Challenger's paragraph 8).

Office Action, pages 3 and 4. Applicant respectfully traverses this rejection.

The burden of establishing a *prima facie* case of obviousness falls on the Examiner.

Ex parte Wolters and Kuypers, 214 U.S.P.Q. 735 (PTO Bd. App. 1979). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). Accordingly, to establish a *prima facie* case, the Examiner must not only show that the combination includes all of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (B.P.A.I. 1985). Further, when prior art references require a selected combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight gained from the invention itself, i.e., something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination. *Uniroyal Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 5 U.S.P.Q.2d 1434 (Fed. Cir. 1988). Because Timson, in view of Challenger, neither includes all elements nor provides a teaching or suggestion to combine, Applicant respectfully asserts that the references fail to establish a *prima facie* case

Serial No. 10/764,918
Amendment and Response to Office Action
Mailed December 8, 2006

of obviousness.

Turning to the claims, amended independent claim 1 recites a method of operating a first security module in a computer comprising, *inter alia*, “detecting a second security module in the computer, wherein *the second security module is of the same type as the first security module.*” (Emphasis added). Amended independent claim 8 recites a first security module comprising “a detector that is adapted to detect another security module *of the same type as the first security module.*” (Emphasis added). Amended independent claim 14 recites a first security module comprising “means for detecting another security module in the computer, wherein *the other security module is of the same type as the first security module.*” (Emphasis added). Amended independent claims 21 and 31 both recite a computer comprising, *inter alia*, “a first security module; and a second security module, wherein *the second security module is of the same type as the first security module.*” (Emphasis added).

In contrast, neither Timson nor Challenger disclose two security modules *of the same type in a computer*. While Timson depicts two security modules, the modules are *of completely different types*. To provide access to secured data, the dual secure data module reader of Timson uses “at least two secure data modules” which “include [1] *an enabling module* and [2] *an interrogatable module.*” (Emphases added). Timson, column 2, lines 16, 20-21. Each type of module performs different distinct functions and both types must be used in conjunction to access secured data. See Timson, column 2, line 13 to column 4, line 15. An enabling module contains “permissions” which determine which data operations, such as “creating data, deleting data, reading data,” etc., may be performed on an interrogatable

Serial No. 10/764,918
Amendment and Response to Office Action
Mailed December 8, 2006

module. Timson, column 2, lines 40-49. In contrast, an interrogatable module contains the operable data. *See* Timson, column 2, lines 50-61. Accessing secured data thus requires (1) permission from an enabling module and (2) operable data from an interrogatable module, where the two different types of modules communicate through a dual secure data module reader. Timson, column 2, line 62 to column 3, line 4; Fig. 1. Accordingly, the dual secure data module reader depicted in Fig. 1 of Timson fails to disclose two security modules *of the same type* in a computer.

Moreover, as discussed in the prior Office Action Response, Challenger fails to disclose multiple security modules of the same type *in a computer*. Since Challenger does not disclose any information that obviates the claimed elements lacking in Timson, the combination of Timson in view of Challenger thus fails to disclose all of the claimed elements. Accordingly, for at least this reason, Applicant respectfully requests withdrawal of the rejection under Section 103.

Even if, assuming *arguendo*, all of the claimed elements were present in Timson in view of Challenger, neither reference provides a teaching or motivation to combine. On the contrary, the references *teach away* from combination. As discussed above, the dual secure data module reader in Fig. 1 of Timson contains two different types of secure data modules including (1) an enabling module and (2) an interrogatable module, each of which must be used in conjunction with the other to encrypt or decrypt data. In other words, a *single secure data module of Timson could not encrypt or decrypt data alone*. *See* Timson, column 2, line 13 to column 4, line 15. In contrast, the Trusted Platform Module of Challenger *requires only*

Serial No. 10/764,918
Amendment and Response to Office Action
Mailed December 8, 2006

a single security module to encrypt or decrypt data. See Challener, paragraph [0006], line 16, to paragraph [0007], line 4. Replacing a Trusted Platform Module with either a single interrogatable module or a single enabling module into the device of Challener would completely disallow the encryption or decryption of data using the device of Challener, negating the very purpose of using a security module. On the other hand, replacing the interrogatable and enabling modules depicted in Fig. 1 of Timson with the Trusted Platform Modules of Challener would similarly defeat the purpose of the dual secure data module reader, which would no longer be necessary if each module could individually encrypt or decrypt data without interacting with another type of module. Because combining Timson and Challener creates a result anathema to the purposes of each disclosed device, rather than provide a motivation to combine, the references *teach away* from combination. Accordingly, without a teaching from the art to combine, the references fail to establish a *prima facie* case of obviousness.


In view of the arguments set forth above, the Applicant respectfully requests that the Examiner withdraw the rejection of independent claims 1, 8, 14, 21, and 31 and provide an indication of allowance. Further, Applicant requests that the Examiner withdraw the rejection of dependent claims 2-7, 9-13, 15-20, 22-26, and 32 based on their respective dependencies and for unique matter recited in each independent claim.

MAR 07 2007

Serial No. 10/764,918
Amendment and Response to Office Action
Mailed December 8, 2006**Conclusion**

The Applicant respectfully submits that all pending claims should be in condition for allowance. However, if the Examiner wishes to resolve any other issues by way of a telephone conference, the Examiner is kindly invited to contact the undersigned attorney at the telephone number indicated below.

Respectfully submitted,

Date: March 7, 2007

Michael G. Fletcher
Registration No. 32,777
(281) 970-4545**Correspondence Address:**IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, CO 80527-2400